This article provides examples of security feature configurations. For details about configuring security-related features on the ACE, see the *Cisco Application Control Engine Module Security Configuration Guide*.

To return to the main article, click here.

# Contents



# Examples of Application Protocol Inspection Configurations

The following examples each illustrate a running-configuration for performing:

- Layer 7 HTTP protocol deep packet inspection
- Layer 7 FTP command inspection
- Layer 3 and Layer 4 DNS application protocol inspection

The application protocol inspection-specific configuration elements appear in bold text in each example.

## Layer 7 HTTP Protocol Deep Packet Inspection

In the following HTTP protocol deep packet inspection configuration, the ACE does the following:

- Includes an ACL that allows the ACE to receive any HTTP traffic through the VLAN.
- Filters on content to allow only HTTL headers that contain the ?html? expression.
- Filters a subset of the HTTP traffic using a content filtering rule that permits the following packet types:
  - ◊ With an HTTP header length greater than 400 bytes
  - ◊ Without the string ?BAD? included in the URL

```
access-list ACL1 extended permit tcp any any eq http

rserver host SERVER1
  ip address 192.168.252.245
  inservice
rserver host SERVER2
  ip address 192.168.252.246
  inservice
rserver host SERVER3
  ip address 192.168.252.247
  inservice

serverfarm host SFARM1
  probe HTTP
  rserver SERVER1
    inservice
  rserver SERVER2
    inservice
  rserver SERVER3
    inservice

class-map match-all L4_FILTERHTTP_CLASS
  2 match access-list ACL1
class-map type http inspect match-all L7_FILTERHTML1_CLASS
  2 match header Accept header-value ?html?
  3 match header length request gt 400
class-map type http inspect match-all L7_FILTERHTML2_CLASS
  2 match url BAD
policy-map type loadbalance first-match L7_HTTP-LB-HTTP_POLICY
  class class-default
    serverfarm SFARM1
policy-map type inspect http all-match L7_FILTERHTML_POLICY
  class L7_FILTERHTML1_CLASS
    permit
  class L7_FILTERHTML2_CLASS
    reset
policy-map multi-match L4_FILTER_POLICY
  class L4_FILTERHTTP_CLASS
    inspect http policy L7_FILTERHTML_POLICY

interface vlan 50
  access-group input ACL1
  ip address 192.168.1.100 255.255.255.0
  service-policy input L4_FILTER_POLICY
  no shutdown
```

## Layer 7 FTP Command Inspection

In the following FTP command inspection configuration, the ACE does the following:

- Masks the responses from the SYST and USER commands
- Denies selected FTP commands from executing
- Allows the remaining FTP commands to execute

```
access-list ACL1 line 10 extended permit ip any any

rserver host SERVER1
  ip address 192.168.252.245
  inservice
```

```
rserver host SERVER2
  ip address 192.168.252.246
  inservice
rserver host SERVER3
  ip address 192.168.252.247
  inservice

serverfarm host SFARM1
  probe FTP
  rserver SERVER1
    inservice
  rserver SERVER2
    inservice
  rserver SERVER3
    inservice

class-map type ftp inspect match-any L7_FTP-MAX-DENY_CLASS
  2 match request-method appe
  3 match request-method cdup
  4 match request-method get
  5 match request-method help
  6 match request-method mkd
  7 match request-method rmd
  8 match request-method rnfr
  9 match request-method rnto
  10 match request-method site
  11 match request-method stou
  12 match request-method cwd
class-map type ftp inspect match-any L7_FTP-MAX-DENY2_CLASS
  2 match request-method syst
  3 match request-method user
class-map match-all L4_FTP-VIP_CLASS
  2 match virtual-address 192.168.120.119 tcp range 3333 4444
policy-map type loadbalance first-match L7_FTP-LB-SF-FTP_POLICY
  class class-default
    serverfarm SFARM1
policy-map type inspect ftp first-match L7_FTP-INSPSF-FTP_POLICY
  class L7_FTP-MAX-DENY_CLASS
    deny
  class L7_FTP-MAX-DENY2_CLASS
    mask-reply
policy-map multi-match L4_VIP_POLICY
  class L4_FTP-VIP_CLASS
    loadbalance vip inservice
    loadbalance policy L7_FTP-LB-SF-FTP_POLICY
    inspect ftp strict policy L7_FTP-INSPSF-FTP_POLICY

interface vlan 29
  ip address 172.16.0.1 255.255.255.0
  fragment chain 20
  fragment min-mtu 68
  nat-pool 1 192.168.120.71 192.168.120.71 netmask 255.255.255.0 pat
  no shutdown
interface vlan 120
  description Upstream VLAN_120 - Clients and VIPs
  ip address 192.168.120.1 255.255.255.0
  fragment chain 20
  fragment min-mtu 68
  access-group input ACL1
  nat-pool 1 192.168.120.70 192.168.120.70 netmask 255.255.255.0 pat
  service-policy input L4_VIP_POLICY
  no shutdown
ip route 10.1.0.0 255.255.255.0 192.168.120.254
ip route 172.16.0.0 255.252.0.0 172.16.0.253
```

### Layer 3 and Layer 4 DNS Application Protocol Inspection

In the following application protocol inspection configuration, the ACE performs DNS query inspection using a Layer 3 and Layer 4 policy map. DNS requires application inspection so that DNS queries will not be subject to the generic UDP handling based on activity timeouts. The ACE performs the reassembly of DNS packets to verify that the packet length is less than the configured maximum length of a DNS reply.

```
access-list ACL1 line 10 extended permit ip any any

class-map match-any L4_DNS-INSPECT_CLASS
  description DNS application protocol inspection of incoming traffic
  match port udp eq domain
policy-map multi-match L4_DNS-INSPECT_POLICY
  class L4_DNS-INSPECT_CLASS
    inspect dns maximum length 1000

interface vlan 70
  ip address 192.168.2.1 255.255.255.0
  access-group input ACL1
  service-policy input L4_DNS-INSPECT_POLICY
  no shutdown
```

## Example of a TCP/IP Normalization and IP Reassembly Configuration

The following example illustrates a running-configuration in which the ACE uses TCP normalization to perform checks for Layer 4 packets that have invalid or suspect conditions and to take the appropriate actions based on the configured TCP connection parameter map settings. The ACE uses TCP normalization to block certain types of network attacks. This configuration also includes IP fragment reassembly parameters. The TCP/IP normalization and IP fragment reassembly configuration appears in bold in the example.

In the following configuration, the ACE does the following:

- Includes a connection parameter map that groups together TCP/IP normalization and termination parameters, such as a connection inactivity timer, ToS for an IP packet, and discarding the SYN segments that contain data. The connection parameter map is associated as an action in the TCP/IP policy map.
- Configures additional IP normalization parameters for a specific VLAN interface, such as clearing all IP options from the packet, define the number of hops that a packet is allowed to reach its destination, and permit the packet with the DF bit set.
- Configures IP fragment reassembly parameters for a specific VLAN interface, such as the minimum fragment size that the ACE accepts for reassembly, the maximum number of fragments that belong to the same packet that the ACE accepts for reassembly, and the minimum fragment size that the ACE accepts for reassembly.

```
access-list ACL1 line 10 extended permit ip any any

parameter-map type connection TCPIP_PARAM_MAP
  set timeout inactivity 30
  set ip tos 20
  tcp-options timestamp allow
  syn-data drop
  urgent-flag clear

class-map match-all L4_TCP_CLASS
  description Filter TCP Connections
```

```
  2 match destination-address 172.27.16.7
  3 match port tcp eq 21
policy-map multi-match L4_TCPIP_POLICY
  class L4_TCP_CLASS
    connection advanced-options TCP_PARAM_MAP

interface vlan 50
  access-group input ACL1
  ip address 192.168.1.100 255.255.255.0
  service-policy input L4_TCPIP_POLICY
  ip ttl minimum 15
  ip options clear
  ip df allow
  fragment size 400
  fragment chain 126
  fragment min-mtu 1024
  fragment timeout 15
  no shutdown

ip route 0.0.0.0 0.0.0.0 192.168.1.0
```

# Examples of NAT Configurations

The following sections show typical scenarios that use dynamic and static NAT solutions:

- Dynamic NAT and PAT (SNAT) Configuration Example
- Server Farm-Based Dynamic NAT (SNAT) Configuration Example
- Static Port Redirection (DNAT) Configuration Example
- SNAT with Cookie Load Balancing Example

## Dynamic NAT and PAT (SNAT) Configuration Example

The following SNAT configuration example shows the commands that you use to configure dynamic NAT and PAT on your ACE. In this SNAT example, packets that ingress the ACE from the 192.168.12.0 network are translated to one of the IP addresses in the NAT pool defined on VLAN 200 by the nat-pool command. The pat keyword indicates that ports higher than 1024 are also translated. If you are operating the ACE in one-arm mode, omit interface VLAN 100 and configure the service policy on interface VLAN 200.

```
access-list NAT_ACCESS line 10 extended permit tcp 192.168.12.0 255.255.255.0 172.27.16.0 255.255.

class-map match-any NAT_CLASS
  match access-list NAT_ACCESS

policy-map multi-match NAT_POLICY
  class NAT_CLASS
    nat dynamic 1 vlan 200

interface vlan 100
  mtu 1500
  ip address 192.168.1.100 255.255.255.0
  service-policy input NAT_POLICY
  no shutdown

interface vlan 200
  mtu 1500
  ip address 172.27.16.2 255.255.255.0
  nat-pool 1 172.27.16.15 172.27.16.24 netmask 255.255.255.0 pat
  no shutdown
```

## Server Farm-Based Dynamic NAT (SNAT) Configuration Example

The following SNAT configuration example shows the commands that you use to configure server farm-based dynamic NAT on your ACE. In this SNAT example, real servers addresses on the 172.27.16.0 network are translated to one of the IP addresses in the NAT pool defined on VLAN 200 by the nat-pool command.

If you are operating the ACE in one-arm mode, omit interface VLAN 100 and configure the service policy on interface VLAN 200.

```
access-list NAT_ACCESS line 10 extended permit tcp 192.168.12.0 255.255.255.0 1 72.27.16.0 255.255

rserver SERVER1
  ip address 172.27.16.3
  inservice
rserver SERVER2
  ip address 172.27.16.4
  inservice

serverfarm SFARM1
  rserver SERVER1
    inservice
  rserver SERVER2
    inservice
class-map type http loadbalance match-any L7_CLASS
  match http content .*cisco.com
class-map match-any NAT_CLASS
  match access-list NAT_ACCESS

policy-map type loadbalance http first-match L7_POLICY
  class L7_CLASS
    serverfarm SFARM1
    nat dynamic 1 vlan 200 serverfarm primary
policy-map multi-match NAT_POLICY
  class NAT_CLASS
    loadbalance policy L7_POLICY
    loadbalance vip inservice

interface vlan 100
  mtu 1500
  ip address 192.168.1.100 255.255.255.0
  service-policy input NAT_POLICY
  no shutdown

interface vlan 200
  mtu 1500
  ip address 172.27.16.2 255.255.255.0
  nat-pool 1 172.27.16.15 172.27.16.24 netmask 255.255.255.0
  no shutdown
```

## Static Port Redirection (DNAT) Configuration Example

The following DNAT configuration example shows those sections of the running configuration related to the commands necessary to configure static port redirection on your ACE. Typically, this configuration is used for DNAT, where HTTP packets that are destined to 192.0.0.0/8 and ingressing the ACE on VLAN 101 are translated to 10.0.0.0/8 and port 8080. In this example, the servers are hosting HTTP on custom port 8080.

```
access-list acl1 line 10 extended permit tcp 10.0.0.0 255.0.0.0 eq 8080 any

class-map match-any NAT_CLASS
```

```
  match access-list acl1

policy-map multi-match NAT_POLICY
  class NAT_CLASS
    nat static 192.0.0.0 255.0.0.0 80 vlan 101

interface vlan 100
  mtu 1500
  ip address 192.168.1.100 255.255.255.0
  service-policy input NAT_POLICY
  no shutdown

interface vlan 101
  mtu 1500
  ip address 172.27.16.100 255.255.255.0
  no shutdown
```

## SNAT with Cookie Load Balancing Example

The following configuration example shows those sections of the running configuration related to the commands necessary to configure SNAT (dynamic NAT) with cookie load balancing. Any source host that sends traffic to the VIP 20.11.0.100 is translated to one of the free addresses in the NAT pool in the range 30.11.100.1 to 30.11.200.1, inclusive. If you want to use PAT instead of NAT, replace ?nat dynamic 1 vlan 2021? with ?nat dynamic 2 vlan 2021? in the L7SLBCookie policy map.

```
server host http
  ip address 30.11.0.10
  inservice
serverfarm host httpsf
  rserver http
    inservice

class-map match-any vip4
  2 match virtual-address 20.11.0.100 tcp eq www
class-map type http loadbalance match-any L7SLB_Cookie
  3 match http cookie JG cookie-value ?.*?

policy-map type loadbalance first-match L7SLB_Cookie
  class L7SLB_Cookie
    serverfarm httpsf
policy-map multi-match L7SLBCookie
  class vip4
    loadbalance vip inservice
    loadbalance L7SLB_Cookie
    nat dynamic 1 vlan 2021

interface vlan 2020
  ip address 20.11.0.2 255.255.0.0
  alias 20.11.0.1 255.255.0.0
  peer ip address 20.11.0.3 255.255.0.0
  service-policy input L7SLBCookie
  no shutdown
interface vlan 2021
  ip address 30.11.0.2 255.255.0.0
  alias 30.11.0.1 255.255.0.0
  peer ip address 30.11.0.3 255.255.0.0
  fragment min-mtu 68
  nat-pool 2 30.11.201.1 30.11.201.1 netmask 255.255.255.255 pat
  nat-pool 3 30.11.202.1 30.11.202.3 netmask 255.255.255.255
  nat-pool 1 30.11.100.1 30.11.200.1 netmask 255.255.255.255
  no shutdown
```